



Cloud Computing Policy

Committee on Information Technology

The National Institute of Standards and Technology (NIST) defines Cloud Computing as: "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Three common service models include, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

CCSF's use of Cloud Computing services must adequately address relevant statutory and policy requirements associated with local government IT systems, including issues of IT security and risk management, privacy, legal issues (e.g., Terms of Service), records management, and other applicable requirements.

Since Cloud Computing can offer benefits in the cost, performance, and delivery of IT services, it is anticipated that the use of Cloud Computing services will grow significantly over the next several years. This policy is intended to ensure that the City takes advantage of Cloud Computing opportunities when appropriate and to ensure the use of these services is managed in accordance with existing COIT policies. (These policies can be found at <http://sfcoit.org/index.aspx?page=4>) The primary reason for this policy is to facilitate a well-managed and successful adoption of Cloud Computing by establishing a process that directs attention to IT-related requirements, management processes, and risk factors.

PURPOSE AND SCOPE

To encourage the use of Cloud Computing, where appropriate, to expedite and reduce the cost of implementing new information technology systems.

This policy pertains to the acquisition of services from a source outside of the CCSF.

POLICY STATEMENT

COIT encourages the use of Cloud Computing where appropriate. To further this policy, departments should consider Cloud Computing options when selecting new information technology systems and soliciting new proposals.

While Cloud Computing may offer advantages in terms of cost and speed of deployment, City departments must also manage risks associated with Cloud Computing.

In assessing the viability of Cloud Computing approaches, departments are encouraged to seek the advice of the City Attorney's office with respect to legal concerns and CIO review with respect to security and technical issues.

COIT Policy Dates

Approved: November 17, 2011
Next Review Date: FY 2017-18



Cloud Computing Policy

Committee on Information Technology

City departments should consider the following concerns, whether the service:

- complies with departmental security and risk management policies;
- complies with all local, State or Federal laws or regulations, including privacy laws, that may govern a department's treatment of data;
- addresses issues of logging, incident reporting, response, forensics, and other security-related functions;
- address disaster recovery and continuity of operations planning;
- clarifies how Personally Identifiable Information (PII) or other sensitive information is involved, and how it will be protected and who is allowed access to it;
- adheres to retention time for all system backups;
- clarifies data ownership and portability;
- considers appropriate data transfer and network capacity requirements.